AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0034] with the following amended paragraph:

[0034] Fig. 1 presents a network overview of the deployment of a T-HA (3) in an enterprise network. It may be deployed connected directly towards the public Internet (2), or located in the DMZ, connected to the Internet, and the Intranet (6), via a firewall (4). The T-HA may alternatively have two separate interfaces for connection to the Internet and the Intranet, not needing for traffic to traverse the firewall again when going entering/exiting the intranet. The Mobile Node (1), in the figure is remotely connecting to the enterprise network, typically over a public access network (e.g. public WLAN hotspot, xDSL, WWAN ...). The Mobile Node tunnels traffic in an encrypted IPSec tunnel within a Mobile IP tunnel (8) (IP or UDP encapsulation) back to the T-HA. The traffic is then forwarded or routed, either directly to its destination (5), or tunneled (9) to the appropriate Internal Home Agent (7), from where it is forwarded to its destination. Traffic in the reverse direction, arrives on the home network for the remotely connected mobile node. The I-HA acts as a proxy for the mobile node, and the traffic is tunneled (IP or UDP encapsulation) back to the T-HA. At the T-HA it is decapsulated and tunneled in an IPSec/Mobile IP tunnel to the Mobile Node.

Please replace paragraph [0044] with the following amended paragraph:

[0044] If the T-HA operation is configured for direct forwarding of traffic from remote users towards their destinations (i.e. T-HA – I-HA encapsulation is 'None'), as shown in Fig. 2, then decapsulated/decrypted packets from the remote user will be routed, using normal IP routing, from the T-HA to their destinations. Where mandatory tunneling is employed between the T-HA and the I-HA for incoming remote connecting MN, as shown in Fig. 3, then the traffic will be encapsulated and forwarded towards the I-HA, at which point, after de-capsulation it will emerge on the home network, appearing like any other traffic originating on this physical network. Where direct forwarding is employed from the T-HA towards its destination, the IP packets may then be filtered by an intervening firewall (3) or similar device. In this way remote access security can be ensured, combined with both internal/external mobility, yet allow the enterprise to apply full packet filtering, in keeping with its enterprise security policies.

Please replace paragraph [0051] with the following amended paragraph:

[0051] Fig. 3 illustrates a Mobile Node connecting from a remote location, towards a T-HA, where tunneling is applied for incoming traffic, from the T-HA to the I-HA. Considering this usage scenario:

- The mobile node connects from a remote location, outside the enterprise network. This connection is typically from a location such as dialup Internet access, public WLAN hotspot, home broadband or another enterprise network.
- A Mobile IP Tunnel is negotiated towards the T-HA, using the T-HA Public IP address as the destination for the mobile IP registration request (RRQ). The NAI and an MD-5 hash of the MN shared secret will be included in this message. Typically in this case there will be no agent discovered by the MN on its local link, thus a colocated registration will be established and the care-of address used by the MN will be that which was assigned in the local access network.
- The T-HA takes the information in the RRQ, and passes the NAI (& potentially the care-of address) towards the RADIUS Server. The RADIUS server will then respond to the T-HA, sending back the T-HA IP Address, I-HA IP Address (both the IP address, (9) in Figure 3 or (10) in Figure 2, visible to the T-HA and the IP address, (10) in Figure 3 or (11) in Figure 2, it has on the Home Network), the MN's Mobile IP shared secret and the MN's IKE shared secret.
- The T-HA will then proceed to authenticate this incoming RRQ, using the shared-secret to generate a MD-5 hash to match against.

- If authentication is successful, a new RRQ is generated by the T-HA for this registration request, and forwarded onwards to the assigned I-HA, using the I-HA Intranet IP address as the destination.
- The I-HA will re-authenticate the request, in a similar way, and will also, if appropriate assign a MN IP address for the MN. This is based on if the MN IP address included in the registration request is 0.0.0.0, and is in accordance with IETF defined procedures for dynamic IP address assignment. After successful authentication, a RRP is sent back to the MN.
- Once the Mobile IP registration is established, IKE negotiation will be initiated from the MN towards the T-HA IP address. During this negotiation, if extended authentication is required, the T-HA may send an XAUTH request message towards the MN requesting additional authentication.
- At the MN, if XAUTH is required, a GUI dialog may be displayed requesting extended credentials entry. These are then sent back to the T-HA in a XAUTH response. At the T-HA authentication is carried out, towards the appropriate external authentication system.
- If successful extended authentication is carried out, then IPSec SA establishment is carried out between the MN and the T-HA, after which traffic can flow.
- The T-HA will maintain a mapping table entry for this MN connection towards the appropriate I-HA.
- Traffic from the Mobile Node will arrive at the T-HA in an IPSec tunnel inside a Mobile IP tunnel (IP or UDP encapsulated). Decapsulation & decryption will take place.
- The mapping table will then be used to determine the treatment of this packet, with it being encapsulated (if appropriate) and forwarded towards the I-HA or forwarded directly towards its destination, in the case where no T-HA – I-HA encapsulation is employed.

- Traffic from the Home Network towards the MN is encapsulated at the I-HA, which proxies on behalf of the remotely located MN on the Home Network (12), and forwarded back to the T-HA.

- At the T-HA, the traffic is decapsulated, and based on the mapping table entry, encrypted and encapsulated toward the MN.